METHOD FOR ENCRYPTED DATA TRANSMISSION VIA A COMMUNICATION NETWORK

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to the German application No. 10330643.9, filed July 7, 2003 and to the International Application No. PCT/EP2004/007378, filed July 6, 2004 which are incorporated by reference herein in their entirety.

FIELD OF INVENTION

[0002] The invention relates to a method for encrypted data transmission as well as to a corresponding computer program product and to a communication system, in particular for the users of an automation system.

BACKGROUND OF INVENTION

[0003] Various methods for encrypted data transmission are known from the prior art. Basically a distinction is made in this field between asymmetrical and symmetrical encryption methods.

[0004] Symmetrical encryption methods are also referred to as "private key" encryption. With a symmetrical encryption method, the users taking part in the communication have the same secret key, which is used both for the encryption and for the decryption. Examples of symmetrical encryption methods known from the prior art are DES, Triple DES, RC2, RC4, IDEA, and Skipjack.

[0005] A common disadvantage of symmetrical encryption methods known from the prior art is that the symmetrical keys must be transmitted to the individual users before the encrypted communication starts, with the possibility that said transmission can be intercepted.

[0006] With asymmetrical encryption methods, which are also referred to as "public key" encryption, a public key is used for the encryption. The data encrypted using the public key of a user can only be decrypted using the secret private key of said user. Known a symmetrical encryption methods are Diffie-Hellmann and RSA.

SUMMARY OF INVENTION

[0007] It is an object of the invention to create an improved encryption method for encrypted data transmission.

[0008] The objects underlying the invention are achieved in each case by the features of the independent claims. Preferred embodiments of the invention are set forth in the dependent claims.

[0009] According to the invention, a symmetrical encryption method is used for the protected data transmission, for example over a public communication network such as the internet. In this case, in contrast to the prior art, the secret symmetrical key is not distributed to the individual users of the communication network, but instead the symmetrical key is generated locally in each case in the individual users.

[00010] Toward that end, data taken from a stochastic process is input into the individual users. On this basis identical symmetrical keys are then generated locally in each case in the users, which keys will henceforward be used for the encrypted data transmission between the users.

[00011] According to a preferred embodiment of the invention the data which forms the basis for the generation of the symmetrical keys in the users is generated by means of a random number generator which uses a stochastic process, such as, for example, thermal (Johnson-Nyquist) noise or a radioactive decay process for the random number generation. Compared to random number generators based on generator polynomials, a random number generator of said kind has the advantage that no pseudo-random numbers are generated. This is because the generator polynomial can in principle be determined by an attacker through analysis of the communication between the users, in particular when cyclical communication is involved.

[00012] According to a further preferred embodiment, at least one measured value is determined from a stochastic process. For example, the data required for generating the symmetrical keys is obtained from the least significant bit positions of the measured value or values.

[00013] According to a further preferred embodiment of the invention, at least one time-variable parameter of an automation system is used as the stochastic process. For this, various measured values supplied, for example, by sensors of the automation system may prove suitable, such as, for example, temperature, speed of rotation, voltage, current, flow rate, velocity, concentration, humidity, etc. The corresponding measured values are stochastic, but can have periodic components, for example. In order to reduce such periodic components, only the least significant bit positions of the measured values, for example, may be used for forming the symmetrical keys.

[00014] According to a preferred embodiment of the invention, stochastic data is acquired by at least two of the users independently of one another. The stochastic data collected by one of the users is transmitted to the other user or users . Overall, each of the users receives all of the stochastic data in this way. The data is then combined in order to obtain a basis for generating the symmetrical key in each particular case.

[00015] According to a further preferred embodiment of the invention, the data which forms the basis for generating the symmetrical key in the users is transmitted over a public network, such as, for example, the internet, or via an Ethernet, for example a LAN, WAN or WLAN.

[00016] According to a further preferred embodiment of the invention, the keys are generated in the users at the request of a master user, the corresponding request being transmitted to the users via the communication network. For example, a corresponding request is made when the utilization of the capacity of the communication network for useful data (payload) transmission is relatively low, in order then to use the unused bandwidth for transmitting data as a basis for the key generation in the users. This approac h is advantageous in particular when the users communicate via the internet.

[00017] If, on the other hand, an Ethernet is used, for example, all the users can "listen in" on the data traffic on the Ethernet. In this case the key generation in the individual use rs can be initiated such that the master user outputs a corresponding trigger command onto the Ethernet.

[00018] According to a further preferred embodiment of the invention, the stochastic data is transmitted and the keys are generated in the users at predeterm ined times or after predetermined time intervals. In this embodiment the users of the communication network have a synchronous time base.

[00019] According to a further preferred embodiment of the invention, different symmetrical encryption methods are used for key generation by the users and corresponding different symmetrical keys generated. For the encrypted data transmission a changeover is effected for example periodically between the encryption methods in order to increase the security of the encrypted data transmission further.

[00020] According to a further preferred embodiment of the invention, the data for the different encryption methods is formed by different combinations of the stochastic data supplied by the individual users.

[00021] The present invention is of particular advantage for use with automation systems. The algorithms for key generation in the individual users can be specified, for example, during the planning and configuration of the system in the project planning phase. The corresponding key generation algorithms are kept secret by the manufacturer of the system. In addition to protection of the encrypted data transmission this also provides protection against the use of unauthorized components, from a third-party manufacturer for example, in the automation system.

[00022] The algorithms are preferably stored in protected memory areas of the automation devices of the automation system, for example in EPROMs or chipcards that are inserted into card readers of the automation devices by authorized users.

[00023] The present invention is particularly advantageously used for components of automation-controlled systems that are linked to one another via public networks. By means of the inventive encrypted data transmission between the users of an automation-controlled system of said kind, unauthorized interventions by third parties are avoided, in particular also when a wireless transmission technology is used between the users.

[00024] According to a further preferred embodiment of the invention, the encrypted data transmission is used for the purposes of remote maintenance or what is referred to as "teleservice" of the system. Here, too, the data transmission method according to the invention offers protection against interception of the transmitted system data or, as the case may be, tampering interventions.

[00025] In addition to an automation-controlled system, the invention can also be advantageously used for the purposes of telecommunication between users or for the purposes of communication between the components of a motor vehicle, shipboard, aircraft or railroad electronics assembly.

BRIEF DESCRIPTION OF THE DRAWINGS

[00026] Preferred embodiments of the invention will be explained in more detail below with reference to the drawings, in which:

[00027] Figure 1 shows a block diagram of a first embodiment of a communication system according to the invention,

[00028] Figure 2 shows a flowchart of a first embodiment of the data transmission method according to the invention,

[00029] Figure 3 shows the generation of data as a basis for generating the key from a measured value,

[00030] Figure 4 shows a block diagram of a further preferred embodiment of a communication system according to the invention,

[00031] Figure 5 shows a block diagram of a preferred embodiment of an automation system according to the invention.

DETAILED DESCRIPTION OF INVENTION

[00032] Figure 1 shows a communication system 100 in which at least the users 102 and 104 can exchange data via a network 106. In a practical embodiment the communication system 100 can include a plurality of users of this kind.

[00033] The users 102, 104 of the communication system 100 each have a prog ram 108 for a symmetrical encryption method. Symmetrical keys can be generated with the aid of the programs 108 on the basis of input data, and useful data to be transmitted can also be encrypted and decrypted.

[00034] The users 102, 104 also each have a memory 110 for storing the symmetrical key generated by the respective program 108.

[00035] The user 102 is connected to an acquisition module 112; said acquisition module 112 serves to collect stochastic data from a stochastic process 114. The stochastic process 114 can be for example the voltage signal of a noisy resistance.

[00036] The user 102 is also connected to a data source 116. Data supplied by the data source 116 is to be transmitted by the user 102 via the network 106 to the user 104.

[00037] During operation of the communication system 100, stochastic data from the stochastic process 114 is recorded by the acquisition module 112. The stochastic data is input into the user 102. The stochastic data is transmitted by the user 102 via the network 106 to the user 104. The transmission can be encrypted or unencrypted.

[00038] The program 108 is started in the user 102 in order to generate a symmetrical key on the basis of the stochastic data supplied by the acquisition module 112, said key being stored in the memory 110. Analogously the program 108 is started in the user 104 in order to use the stochastic data received via the network 106 from the user 102 for generating the same symmetrical key which is stored in the memory 110 of the user 104.

[00039] If further users are present in the c ommunication system 100, said further users also receive the stochastic data from the user 102 via the network 106 and in each case generate the symmetrical key locally with the aid of the respective program 108.

[00040] Data which is supplied to the user 102 by the data source 116 can now be transmitted in encrypted form via the network 106 to the user 104. Toward that end the useful data to be transmitted is encrypted with the aid of the program 108 of the user 102 and the symmetrical key stored in the memory 110 of the user 102.

[00041] The encrypted useful data is transmitted via the network 106 and received by the user 104. There, the data is decrypted by the program 108 of the user 104 with the aid of the symmetrical key stored in the memory 110 of the user 104.

[00042] The generation of the stochastic data as a basis for generating the symmetrical keys in the users 102, 104 can be performed here by a stochastic random number generator which uses, for example, the output voltage of a noisy resistance as the stochastic pr ocess.

[00043] Alternatively, the data supplied by the data source 116 can also be used as stochastic data as a basis for generating the symmetrical key. This is advantageous in particular when the data source 116 supplies measured values of quantities or parameters that vary over time, of an automation system for example. For example, certain process parameters in an automation system of said kind, such as the temperature, pressure, speed of rotation, etc., are not deterministic, but more or less random with more or less periodic components. A corresponding measured value supplied by the data source 116 can the refore be used as a stochastic datum for symmetrical key generation, a separate acquisition module 112 or, as the case may be, an additional stochastic process 114 being superfluous in this case.

[00044] Figure 2 shows a corresponding flowchart. Stochastic data is acquired in step 200. In this case said data can be stochastic data supplied by a random number generator or the useful data supplied by a data source. The stochastic data is transmitted to the users of the communication system in step 202. This transmi ssion can take place in encrypted or unencrypted form over a public network.

[00045] In step 204, identical symmetrical keys are generated locally in each case by the users on the basis of the stochastic data. For this purpose use is made of a secret encryption method which is implemented in each case in the users by means of a computer program.

[00046] Each of the users that received the stochastic data in step 202 therefore inputs said stochastic data into the computer program in order to generate a symmetrical key w hich is stored locally by the respective user.

[00047] As a result all the users therefore have the symmetrical key without this having been transmitted over the network 106. Even by eavesdropping on the transmission of the stochastic data via the network 106, a third party cannot come into possession of the key, since the secret encryption method or, as the case may be, the corresponding computer program is required for this. In order to avoid unauthorized accesses to the computer program this is preferably stored in a protected memory area, for example in an EPROM or on a chipcard.

[00048] After the identical symmetrical keys based on the stochastic data have been generated in the individual users, said keys are used for the protected communication between the users in step 206.

[00049] Figure 3 shows an exemplary embodiment for generating stochastic data as a basis for generating the symmetrical keys. For example, a measured value 300 having a length of, for example, 32 bits is supplied by the data source 116 (cf. Figure 1) . Only the eight least significant bit (LSB) positions of the measured value 300, for example, are used for generating the keys.

[00050] In other words, therefore, the least significant bit positions of the measured value 300 form the stochastic data that is used for generating the keys. In this case the use of only the least significant bit positions of the measured value 300 has the advantage over the use of the full measured value 300 or of only the most significant bit (MSB) positions that periodic components of the measured signal are reduced or eliminated.

[00051] Figure 4 shows a block diagram of a communication system 400. Elements of Figure 4 that correspond to elements of the embodiment shown in Figure 1 are identified by means of reference numerals increased by 300.

[00052] In the embodiment according to Figure 4, the user 402 is connected to the data sources 418 and 420 which continuously supply the measured values a and b. The user 404 is connected to the data source 422 which continuously supplies the measured va lue c. The measured value a is, for example, a temperature, the measured value b a rotary speed, and the measured value c a pressure.

[00053] The users 402 and 404 each have a memory 424 for storing the measured values a, b and c. In addition, the users 402 and 404 each have a memory 426 for storing the symmetrical keys S1 and S2. The key S1 is generated by the program 408 on the basis of a combination of the measured values a and c and the key S2 on the basis of the measured values a and b.

[00054] During operation of the communication system 400, the symmetrical keys S1 and S2 are generated in the users 402 and 404 as well as in further essentially identically structured users.

[00055] For this purpose the measured values a, b and c output at a given moment in time by the data sources 418, 420, 422 are stored in the memory 424. That is to say, the user 402 stores the measured values a and b in its memory 424 and transmits said values over the network 406 to the further users, i.e. in particular to the user 404, where the mea sured values a and b are also stored in the memory 424.

[00056] On the other hand the user 404 stores the measured value c in its memory 424 and transmits the measured value c over the network 406 to the other users, i.e. in particular to the user 402, where the measured value c is also stored in the respective memory 424. As explained with reference to Figure 3, preferably only the least significant bit positions are stored in the memories 424 in place of the full measured values.

[00057] The program 408 of the user 402 combines the measured values a and b which are stored in the memory 424 or, as the case may be, the least significant bit positions of said measured values with one another, for example by appending the corresponding bits to one another. The data word resulting from this is used by the program 408 for generating the key S2.

[00058] Analogously, the key S1 is generated with the aid of the program 408 on the basis of the measured values a and c. The keys S1 and S2 are stored in the memory 426 of the user 402. The same operation in principle is run in the user 404 as well as in the further users of the communication system 400, with the result that the keys S1 and S2 are present in all users.

[00059] Subsequently, an encrypted transmission of the measured values a, b and c takes place over the network 406, with the key S1 being used for the encrypted data transmission at specific times and the key S2 being used for the encrypted data transmission at specific times. These times can be predefined or event-driven. For example, one of the users can assume the function of a master user for initiating the key generation or for switching over between the keys in the different users.

[00060] In the exemplary embodiment considered here, therefore, the measured values a, b and c are used to form different data words by means of a predefined combinatorial mechanism, which data words for their part are the basis for generating different symmetrical keys. Said combinatorial mechanism can be invariable over time or variable over time.

[00061] Figure 5 shows an automation system 500 comprising the automation devices 502, 504, 506, 508, 510 and 512. The automation devices 502 through 512 are interconnected by means of a data bus 514. This can be, for example, an Ethernet. A further automation device 516 can exchange data via a public network 518 such as, for example, the internet or a wireless mobile radio link.

[00062] Each of the automation devices 502 through 512 and 516 has an encryption program 520 and an encryption program 522. Further encryption programs may also be present. The encryption programs 520 and 522 each provide different symmetrical encryption methods.

[00063] In addition, each of the automation devices 502 through 512 and 516 has a timer 524. The timers 524 are synchronized with one another, so a uniform synchronous time base is created for the automation system 500.

[00064] Each of the automation devices 502 through 512 also has a memory 526 and a memory 528. The memory of the automation device 502 is used for storing the "Value 1" which is output by a corresponding measured value sensor 1. The memory 528 of the automation device 502 is used for storing the "Value 5" which is output by a measured value sensor 5. The situation is analogous for the memories 526 and 528 of the further automation devices 504 through 512, each of which is assigned to specific measured value sensors, as can be seen from Figure 5. For the sake of clarity, the measured value sensors are not shown in Fig. 5.

[00065] The data word which serves as a basis for generating a symmetrical key is generated by means of a predefined combinatorial mechanism, for example from the concatenation of the values 1, 2, 3 and 4. The data word obtained by means of said concatenation is in each case input into the encryption programs 520 and 522 in order to generate corresponding symmetrical keys.

[00066] For the encrypted data transmission between the automation devices 502 through 512 and 516, the encryption programs 520 and 522 are used in a preconfigured chronological sequence, i.e. it is pre-planned for each instant in time whether the encryption program 520 or 522 is to be used for the encrypted data transmission.

[00067] The automation device 516 is, for example, a remote maintenance device. The automation device 516 also receives the measured values 1, 2, 3 and 4 via the network 518 in order to compute the respective keys with the aid of the encryption programs 520 and 522. The measured values are transmitted in this case by the automation devices 502, 504 and 510 via the data bus 514 and the network 518 to the automation device 516. After the key generation has been completed, remote maintenance can be performed by the automation device 516, the data transmitted over the network 518 during this activity being protected against interception and manipulation.

[00068] The network has the network access points 530 and 532 via which the data traffic flows between the data bus 514 and the automation device 516. For the transmission over the network 518, a further encryption can be performed by encrypting the already encrypted data a second time. By this means security against external attacks is further increased.

[00069] This is advantageous in particular when the network 518 is a public network. The further encryption for the transmission over the network 518 can be performed analogously to that shown in Figure 1, with the network access point 530 taking on the role of the user 102 and the network access point 532 the role of the user 104.

[00070] It is of particular advantage that the protected data transmission between the automation devices is handled independently of general security infrastructures, such as, for example, central trust centers, but is based on data which is variable over time and originates from the system itself. It is of further advantage that an implicit authentication of the automation devices is also carried out as a result of the secret encryption programs 520, 522. Unauthorized automation devices for which the system is not approved or automation devices from third-party manufacturers that do not have the requisite licenses do not have the secret encryption programs 520, 522 and consequently also cannot be used in the automation system.

[00071] In order to increase security further, a list of encryption programs can be loaded in each of the individual automation devices. Said encryption programs are preferably loaded during offline operation of the automation system in order to avoid the encryption programs being spied on. The encryption programs are stored for example in protected memory areas of EPROMs or chipcards.

[00072] The changeover times for switching between the encryption programs and the associated keys can be determined on a command-controlled basis by one of the automation devices, which device thereby assumes the function of a master. Alternatively, the changeover times can be configured in advance by means of predefined absolute times or programmed on a cyclical or periodic basis.

[00073] Alternatively, an algorithm fed by random values of the system can be used for specifying the changeover times. A further possibility is that the utilization of the data bus 514 is monitored and the key generation or, as the case may be, changeover between the encryption programs initiated at a time when the utilization level of the data bus 514 is low. This has the advantage that unused bandwidth of the data bus 514 can be used for transmitting the measured values to the individual automation devices.